Brandon Rollinson Jr

11/14/2025

Cybersecurity Analyst- Social Science foundations in Cyber Defense

Introduction

Being in this cybersecurity field it's often viewed as a purely technical field but that is false. Most essential tasks depend on the understanding of human behavior, social systems, and the social forces that can definitely shape how the users interact with technology. Doing my research and finding a field that I want to pursue within cyber security is a Cybersecurity Analyst. This is one of the most critical roles in the industry and this field depends on social science because you have to understand how individuals, organizations, and broader society react to threats. As you apply different concepts like socialization, cultural norms, and human decision making will allow an analyst to identify the vulnerabilities that come not from the computer but from people. In this paper I will be mentioning how cybersecurity analysts rely on social science principles in their work force and the responsibilities.

Understand Human Behavior in Threat Detection

Cybersecurity analysts are always monitoring user activity and system alerts. Behavioral psychology plays a big role and you need a good understanding. This is why users fall for phishing, clicking on harmful links, reuse passwords, or ignore warnings. As I did my research it shows that optimism bias, authority bias, and habituation influences digital decision-making

(Haldington,2017). Analysts stick to these principles when they try to determine if an unusual login pattern is a sign of intrusions.

Human Factors and Social Engineering Defense

An important thing to remember is that cybersecurity analysts prevent social engineering attacks. You must understand organizational sociology and how workplace culture, group norms, communication structures, and leadership affect the employees behavior. In the research it demonstrates that organizations that have poor communication or weak training experience a higher rate of social engineering success(D'Arcy & Greene, 2014). They use this knowledge to create realistic phishing simulations, make behavioral risk assessments, and develop communication strategies that reinforce secure habits. A lot of analysts use the social science survey method.

Interaction With Marginalized Groups

The cybersecurity policies might unintentionally create a barrier for marginalized populations and an analyst's security decisions can impact low income users, people with disabilities, immigrants, communities with limited digital literacy. If you apply social science principles it can help the analyst recognize all of these impacts. A human center design can uplift them and create solutions that could be accessible, sensitive, and equitable. A good example would be offering an authentication option, security language, or providing a multilingual training that makes sure all groups can engage with technology safely.

Conclusion

Overall, as you can tell from my research, a cybersecurity analyst blends in with technical skills that go in depth with social science knowledge. An analyst relies on psychology and this helps understand user behavior, sociology , criminology to interpret threats, and human center design to make sure equitable access to security. The role impacts marginalized groups and society as a whole, this makes social science essential for ethical and effective cyber defense. Cyber threats grow more complex, reliance on social science increases, Cybersecurity analysts being at the forefront of technology.

Cites

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589

D'Arcy, J., & Greene, G. (2014). Security culture and the prevention of insider threats. *Information Systems Journal, 24*(2), 128–157. https://doi.org/10.1111/isj.12053

Hadlington, L. (2017). Human factors in cybersecurity: Examining the role of human behavior in information security. *Computers & Security, 68*, 94–105. https://doi.org/10.1016/j.cose.2017.04.004